日本国特許庁
JAPAN PATENT OFFICE

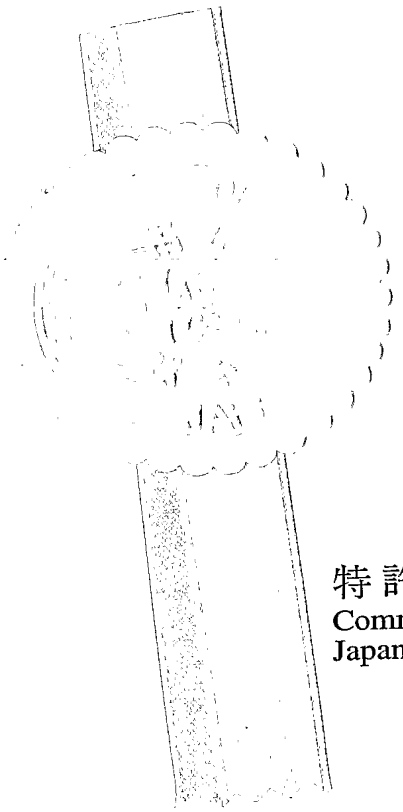
23. 4. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１２月２６日

出願番号
Application Number: 特願２００３－４３２４４７
[ST. 10/C]: [ＪＰ２００３－４３２４４７]

出願人
Applicant(s): 三菱電機株式会社



２００４年 ６月 ４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号 出証特２００４－３０４８２２４

【書類名】　特許願
【整理番号】　548698JP01
【提出日】　平成15年12月26日
【あて先】　特許庁長官殿
【国際特許分類】　G09F 15/00
【発明者】
　【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
　【氏名】　大越　丈弘
【発明者】
　【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
　【氏名】　山田　敬喜
【発明者】
　【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
　【氏名】　牧田　覚
【特許出願人】
　【識別番号】　000006013
　【氏名又は名称】　三菱電機株式会社
【代理人】
　【識別番号】　100099461
　【弁理士】
　【氏名又は名称】　溝井　章司
【手数料の表示】
　【予納台帳番号】　056177
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、
上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持していない場合に新たな認証用鍵を生成し、上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持している場合で上記認証処理部による上記被認証装置との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部とを備え、
上記認証処理部は、上記更新鍵生成部により生成された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする認証装置。
【請求項２】
上記認証装置は、さらに、
被認証装置から所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部を備え、
上記更新鍵生成部は、上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記新たな認証用鍵を生成し、
上記認証装置は、さらに、
上記更新鍵生成部により生成された新たな認証用鍵を被認証装置に送信する送信部を備え、
上記認証処理部は、上記送信部により送信された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする請求項１記載の認証装置。
【請求項３】
所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する記憶部と、
認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、
上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信する送信部と、
上記認証装置から上記送信部により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいた新たな認証用鍵を受信する受信部と
を備え、
上記認証処理部は、上記受信部により受信された新たな認証用鍵を用いて上記認証装置との間での認証処理を再度おこなうことを特徴とする被認証装置。
【請求項４】
上記受信部は、上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記認証装置から所定の情報を受信し、
上記送信部は、上記受信部により所定の情報が受信された場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信することを特徴とする請求項３記載の被認証装置。
【請求項５】
所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信する第１の送信工程と、
上記第１の送信工程により上記認証装置から送信された所定の情報を上記被認証装置が受信する第１の受信工程と、
上記第１の受信工程により上記所定の情報が受信された後、上記被認証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信する第２の送信工程と、
上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置が受信する第２の受信工程と、
上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子

とに基づいて、上記認証装置が新たな認証用鍵を生成する生成工程と、
上記生成工程により生成された新たな認証用鍵を被認証装置に送信する第３の送信工程と、
上記第３の送信工程により送信された新たな認証用鍵を上記被認証装置が受信する第３の受信工程と、
上記第３の受信工程により受信された新たな認証用鍵を、上記被認証装置と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこなう鍵更新工程と、
更新確認データを生成して上記認証装置へ送信する工程と、
更新確認データを受信し、確認する工程と
を備えたことを特徴とする鍵更新方法。

【書類名】明細書
【発明の名称】認証装置及び被認証装置及び鍵更新方法
【技術分野】
【０００１】
本発明は、認証装置、被認証装置、或いは両者の鍵更新方法に関する。特に、ＥＴＣ（ノンストップ自動料金支払いシステム）やドライブスルー等、無線通信機能を有する移動体及び移動体通信システムに関する。
【背景技術】
【０００２】
利用者があるサービスを受けるとき、サービスを受けられる正当な利用者であるか本人確認（認証）が行われる。その際、鍵なし・期限切れ等の理由により認証に失敗するとサービスを受けることができない。
【特許文献１】特開２００３－１９６２４０号公報
【特許文献２】特開平１１－２７４９９９号公報
【特許文献３】特開２０００－１３８６７４号公報
【特許文献４】特開２０００－１９６５８８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
利用者は、鍵の更新等正当な利用者であるための手続きを怠ると、たとえ正当な利用者であっても（不正を行う意図はなくとも）、サービスを受けることができなくなるといった問題があった。
【０００４】
また、上記特許文献１に記載の技術では、テンポラリで認証が許可されてしまうため、過去に認証に成功していれば、その後何度でも認証されてしまい、認証装置にアクセス可能となることからセキュリティホールになりかねないといった問題があった。
【０００５】
また、上記特許文献２～４に記載の技術では、双方が保持している鍵の中から、使用鍵を決定しているに過ぎず、鍵更新をおこなうことができないといった問題があった。
【０００６】
本発明は、鍵更新をおこなうことで更新された鍵により正当な利用者に対しては、サービスを提供し、サービスの可用性及び利用者の利便性を向上させることを目的とする。
【課題を解決するための手段】
【０００７】
この発明に係る認証装置は、認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、
上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持していない場合に新たな認証用鍵を生成し、上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持している場合で上記認証処理部による上記被認証装置との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部とを備え、
上記認証処理部は、上記更新鍵生成部により生成された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする。
【発明の効果】
【０００８】
本発明によれば、鍵なし・期限切れ等の場合であっても鍵の更新をおこなうことができ、その後に正当な利用者がサービスの提供を受けることができ、本発明を利用するシステムのサービスの可用性及び利用者の利便性を向上させることができる。
【発明を実施するための最良の形態】
【０００９】

実施の形態１．
以下に説明するように、被認証装置と認証装置との間での認証時、被認証装置が鍵なし又は被認証装置が有する鍵が有効期限切れであっても、認証失敗とするのではなく、鍵更新手段により鍵更新を実施し、その後、認証を行うものである。
【００１０】
図１は、実施の形態１における認証システムの構成を示す図である。
【００１１】
図１において、認証システムは、認証装置となる通信装置１００と被認証装置となる通信装置２００とを備えている。通信装置１００は、アンテナ１０１、通信処理部１１０、記憶部１２０、制御部１３０、更新処理部１９６、認証処理部１９７を備えている。通信処理部１１０は、受信部１１１、送信部１１２を有している。更新処理部１９６は、暗号処理部１４０、乱数生成部１５０、更新鍵生成部１６０、個別鍵生成部１７０、一時鍵生成部１８０、更新用データ生成部１９０、更新確認データチェック部１９５を有している。通信装置２００は、アンテナ２０１、通信処理部２１０、記憶部２２０、制御部２３０、更新処理部２９６、認証処理部２９７を備えている。通信処理部２１０は、受信部２１１、送信部２１２を有している。更新処理部２９６は、暗号処理部２４０、乱数生成部２５０、一時鍵生成部２８０、更新用データチェック部２９０、更新確認データ生成部２９５を有している。実施の形態１では、通信装置１００と通信装置２００とは、アンテナ１０１，２０１を介して無線通信する場合を説明するが、これに限るものではなく有線通信であっても構わない。例えば、ＥＴＣ（料金自動収集）、ドライブスルー等において、通信装置１００は、店舗側の路側機として、通信装置２００は、自動車側の車載機として構成される。
【００１２】
図２は、実施の形態１における認証システムの概念を示す図である。
【００１３】
例えば、ＥＴＣ、ドライブスルー等において、通信装置１００は、店舗側の路側機として、通信装置２００は、自動車側の車載機として構成される場合、ＥＴＣ、ドライブスルー等によるサービス提供において、店舗側の路側機は、起動後、認証処理を実施する状態で、利用者（自動車）の来店（通過）を待ち続ける。
【００１４】
利用者が来店すると、路側機は自動車に設置された車載機に対して認証要求を送信する。
【００１５】
車載機は路側機の指示にしたがって必要な情報を路側機に送信する。
【００１６】
路側機は、車載機から受け取った情報が古い或いは鍵がないと判断した場合、鍵更新の状態となり、車載機に対して鍵更新要求を実施する。
【００１７】
車載機は、路側機の指示にしたがって鍵更新を実施する。
【００１８】
鍵更新終了後、路側機は認証状態となり、車載機に対して認証処理を実施する。
【００１９】
言い換えれば、本実施の形態１における認証システム或いは認証方式は、鍵更新手段を備えている。そして、認証処理と更新処理が分離している。認証処理中は、更新処理はされない。
【００２０】
そして、鍵情報が古い又はない場合、鍵更新を実施してから認証処理を実施する。すなわち、初期時（鍵情報がないとき）、鍵更新処理を実施する。或いは、通常運用時は認証処理を実施して、認証に用いる鍵情報が古い場合、鍵更新処理を実施する。
【００２１】

図３は、実施の形態１における鍵更新方法の手順を示すフローチャート図である。

【００２２】

記憶部１２０は、所定のアルゴリズム識別子と所定の暗号鍵識別子と、上記所定のアルゴリズム識別子に対応するアルゴリズムを記憶している。

【００２３】

記憶部２２０は、所定のアルゴリズム識別子と所定の暗号鍵識別子と、上記所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵と装置固有番号とを記憶している。また、上記記憶部２２０は、古くなった或いは使用期限が過ぎた認証用鍵及びその認証用鍵の識別子を記憶している。或いは、記憶部２２０は、認証用鍵を記憶していない場合であってもよい。ここで、所定の暗号鍵識別子は、鍵更新専用の鍵の識別子（更新用識別子）である。所定の暗号鍵識別子に対応する暗号鍵は、鍵更新専用鍵である。この鍵更新専用の鍵の識別子及び鍵更新専用鍵は、初期時（例えば装置の出荷時）における新規鍵生成に伴う鍵更新処理、或いは通常運用時に発生した鍵更新処理において、通信装置１００，２００間で互いに共有できる認証用鍵が存在しない緊急時における別の新たな鍵生成に伴う鍵更新処理のいずれかの場合に用いる。認証処理に用いることはない。

【００２４】

まず、認証処理部１９７は、被認証装置となる通信装置２００との間で認証処理をおこなう。言い換えれば、認証処理部２９７は、認証装置となる通信装置１００との間で認証処理をおこなう。認証処理の際、認証用鍵を用いておこなう。ここで、記憶部２２０が、古くなった或いは使用期限が過ぎた認証用鍵を記憶している場合、或いは、記憶部２２０が、認証用鍵を記憶していない場合、認証用鍵が使用できないので、ここでの認証処理は失敗に終わることになる。

【００２５】

Ｓ（ステップ）２０１において、乱数生成工程として、上記認証処理が失敗に終わると、乱数生成部１５０は、乱数１を生成する。

【００２６】

Ｓ２０２において、送信工程として、送信部１１２は、乱数生成部１５０により生成された乱数１（所定の情報の一例である）を通信情報１として通信装置２００に送信する。通信装置１００は、乱数１を通信情報１として通信装置２００に送信することで、認証処理から鍵更新処理に移行したことを通信装置２００へ知らせることになる。

【００２７】

Ｓ２０３において、受信工程として、受信部２１１は、送信部１１２により送信された乱数１を通信情報１として受信する。通信装置２００では、受信部２１１が、乱数１を受信したことにより、通信装置１００より鍵更新が要求されたと判断する。

【００２８】

Ｓ２０４において、認証処理工程の一部として、乱数生成部２５０は、乱数２を生成する。

【００２９】

Ｓ２０５において、送信工程として、送信部２１２は、上記記憶部２２０により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子と装置固有番号と、乱数生成部２５０により生成された乱数２とを通信情報２として認証装置である通信装置２００に送信する。存在する場合には、古くなった或いは使用期限が過ぎた認証用鍵の識別子と対応するアルゴリズムの識別子とを一緒に送信する。ここで、１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組みとしてプロファイルとして表し、通信情報２は、乱数２と装置固有番号と組数分のプロファイル数とプロファイル数分の各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とをデータとして有している。さらに、ここでは、各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とを対応させたデータとしている。言い換えれば、上記送信部２１２は、上記記憶部２２０により１つのア

ルゴリズム識別子と１つの暗号鍵識別子とを１組のプロファイルとして記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置となる通信装置１００に送信する。

【００３０】

Ｓ２０６において、受信工程として、受信部１１１は、被認証装置となる通信装置２００から、乱数２と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも１つのプロファイル識別子と少なくとも１つのプロファイル識別子の各プロファイル識別子に対応した少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを有する通信情報２を受信する。

【００３１】

Ｓ２０７において、生成工程として、更新鍵生成部１６０は、上記受信部１１１により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記鍵更新専用の鍵の識別子である所定の暗号鍵識別子と所定の暗号鍵識別子に対応する上記所定のアルゴリズム識別子とを選択する。そして、更新鍵生成部１６０は、上記受信部１１１により受信された装置固有番号等とたとえばハッシュ値等を用いて更新鍵となる新たな認証用鍵を生成する。言い換えれば、更新鍵生成部１６０は、上記受信部１１１により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記認証処理部１９７による認証処理に用いる認証用鍵を上記被認証装置となる通信装置２００が保持していない場合に新たな認証用鍵を生成し、上記認証処理部１９７による認証処理に用いる認証用鍵を上記被認証装置となる通信装置２００が保持している場合で上記認証処理部１９７による上記被認証装置となる通信装置２００との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する。

【００３２】

Ｓ２０８において、個別鍵生成工程として、個別鍵生成部１７０は、上記更新鍵生成部１６０により選択された所定の暗号鍵識別子に対応する暗号鍵となる通信装置２００が有している鍵更新専用鍵となる個別鍵を更新鍵生成部１６０と同様の方法で生成する。

【００３３】

Ｓ２０９において、一時鍵生成工程として、一時鍵生成部１８０は、上記更新鍵生成部１６０により選択された所定のアルゴリズム識別子に対応するアルゴリズムを用いて所定の暗号鍵識別子に対応する暗号鍵となる個別鍵生成部１７０により生成された個別鍵で乱数１，２を暗号処理部１４０を用いて暗号化し、鍵更新処理用暗号鍵の一例となる一時鍵を生成する。

【００３４】

Ｓ２１０において、更新用データ生成工程として、更新用データ生成部１９０は、乱数２のすべて或いは一部と、更新鍵となる新たな認証用鍵とを暗号処理部１４０により一時鍵生成部１８０により生成された一時鍵で暗号化することにより更新用データを生成する。

【００３５】

Ｓ２１１において、送信工程として、送信部１１２は、上記更新鍵生成部１６０により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のプロファイル識別子と更新用データ生成部１９０により生成された更新用データとを通信情報３として上記被認証装置となる通信装置２００に送信する。

【００３６】

Ｓ２１２において、受信工程として、受信部２１１は、上記認証装置となる通信装置１００から上記送信部２１２により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のアルゴリズム識別子と所定の暗号鍵識別子とに対応するプロファイル識別子と更新用データとを通信情報３として受信する。言い換えれば、上記受信部２１１は、上記認証装置となる通信装置１００から上記送信部２１２により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいた新たな認証用鍵を受信する。

【００３７】

Ｓ２１３において、確認工程として、暗号処理部２４０は、受信部２１１により受信されたプロファイル識別子を確認し、プロファイル識別子に対応する所定の暗号鍵識別子と所定のアルゴリズム識別子とを確認する。

【００３８】

Ｓ２１４において、一時鍵生成工程として、一時鍵生成部２８０は、受信部２１１により受信され、暗号処理部２４０により確認された所定のアルゴリズム識別子に対応するアルゴリズムを用いて、記憶部２２０に記憶された個別鍵で乱数１，２を暗号処理部２４０を用いて暗号化し、更新処理用暗号鍵の一例となる上記一時鍵を生成する。以上により通信装置１００，２００間で同じ一時鍵という鍵共有ができたことになる。なお、この実施形態では、一時鍵生成部１８０，２８０が一時鍵生成の際、個別鍵で暗号化したが、認証装置と被認証装置とが同じ処理を実施すればよいため、復号してもよい。

【００３９】

Ｓ２１５において、更新用データチェック工程として、更新用データチェック部２９０は、受信部２１１により通信情報３として受信された暗号化されている更新用データを一時鍵生成部２８０により生成された一時鍵により暗号処理部２４０を用いて復号する。

【００４０】

Ｓ２１６において、鍵更新工程の一部として、更新用データチェック部２９０は、復号した更新用データのデータが、通信装置２００が通信装置１００に送信した乱数２のすべて或いは一部であるかどうかを確認する。復号した更新用データのデータが乱数２のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置１００との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置１００，２００間での認証処理の一方が成功したことを意味する。そして、更新用データチェック部２９０は、復号することによって得られた上記受信部２１１により受信された新たな認証用鍵を、上記通信装置１００と通信装置２００との間での認証処理をおこなうための更新鍵として鍵更新をおこなう。更新鍵は、記憶部２２０に記憶される。

【００４１】

Ｓ２１７において、更新確認データ生成工程として、更新確認データ生成部２９５は、乱数１のすべて或いは一部を暗号処理部２４０により一時鍵生成部２８０により生成された一時鍵で暗号化することにより更新確認データを生成する。

【００４２】

Ｓ２１８において、送信工程として、送信部２１２は、更新確認データ生成部２９５により生成された更新確認データを通信情報４として通信装置１００に送信する。

【００４３】

Ｓ２１９において、受信工程として、受信部１１１は、通信装置２００から更新確認データを通信情報４として受信する。

【００４４】

Ｓ２２０において、更新確認データチェック工程として、更新確認データチェック部１９５は、受信部１１１により通信情報４として受信された暗号化されている更新確認データを一時鍵生成部１８０により生成された一時鍵により暗号処理部１４０を用いて復号する。

【００４５】

Ｓ２２１において、更新確認データチェック工程として、更新確認データチェック部１９５は、復号した更新確認データのデータが、通信装置１００が通信装置２００に送信した乱数１のすべて或いは一部であるかどうかを確認する。復号した更新確認データのデータが乱数１のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置２００との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置１００，２００間での認証処理の他方が成功したことを意味する。

【００４６】

以上により、通信装置１００，２００間での鍵更新処理が終了し、その後、上記認証処理部１９７は、上記更新鍵生成部１６０により生成された新たな認証用鍵を用いて上記被

認証装置となる通信装置２００との間での認証処理を再度おこなう。言い換えれば、上記認証処理部２９７は、上記受信部２１１により受信された新たな認証用鍵を用いて上記認証装置となる通信装置１００との間での認証処理を再度おこなう。

【００４７】

図４は、通信情報１のフレームの一例を示す図である。

【００４８】

図４において、通信情報１は、ヘッダと乱数１データを有している。

【００４９】

図５は、通信情報２のフレームの一例を示す図である。

【００５０】

図５において、通信情報２は、ヘッダと乱数２データと装置固有番号（装置固有Ｎｏ．）とプロファイル数（Ｐｒｏｆｉｌｅ数）と各プロファイルを識別するプロファイル識別子としてのＰｒｏｆｉｌｅ１，・・・Ｐｒｏｆｉｌｅ　ｎと、各プロファイル識別子に対応するアルゴリズム識別子（アルゴリズムＩＤ）と暗号鍵識別子（鍵ＩＤ）とを有している。プロファイルの最終番号に鍵更新専用の鍵の識別子（更新用識別子）と更新用識別子に対応するアルゴリズム識別子が記載されている。図５では、各プロファイル識別子と各プロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

【００５１】

図６は、通信情報３のフレームの一例を示す図である。

【００５２】

図６において、通信情報３は、ヘッダと選択された所定のプロファイルを識別する所定のプロファイル識別子としてのＰｒｏｆｉｌｅ　ｎと、所定のプロファイル識別子に対応するアルゴリズム識別子（アルゴリズムＩＤ）と暗号鍵識別子（鍵ＩＤ）と更新用データとを有している。図５では、所定のプロファイル識別子と所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

【００５３】

図７は、通信情報４のフレームの一例を示す図である。

【００５４】

図７において、通信情報４は、ヘッダと更新確認データとを有している。

【００５５】

ここで、制御部１３０は、通信装置１００の各部を制御する。また、制御部２３０は、通信装置２００の各部を制御する。また、記憶部１２０は、通信装置１００の各部で行なわれる処理中に生じるデータを記憶する。また、記憶部２２０は、通信装置２００の各部で行なわれる処理中に生じるデータを記憶する。

【００５６】

以上のように、本実施の形態１における鍵更新方法は、所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信する第１の送信工程と、上記第１の送信工程により上記認証装置から送信された所定の情報を上記被認証装置が受信する第１の受信工程と、上記第１の受信工程により上記所定の情報が受信された後、上記被認証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信する第２の送信工程と、上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置が受信する第２の受信工程と、上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記認証装置が新たな認証用鍵を生成する生成工程と、上記生成工程により生成された新たな認証用鍵を被認証装置に送信する第３の送信工程と、上記第３の送信工程により送信された新たな認証用鍵を上記被認証装置が受信する第３の受信工程と、上記第３の受信工程により受信された新たな認証用鍵を、上記被認証装置

と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこなう鍵更新工程と、更新確認データを生成して上記認証装置へ送信する工程と、更新確認データを受信し、確認する工程とを備えている。

【００５７】

また、例えば、ＥＴＣ、ドライブスルー等において、通信装置１００は、店舗側の路側機として、通信装置２００は、自動車側の車載機として構成される場合、以上のように、この認証方式を実施する車載機は、路側機からの指示に従って鍵更新へ状態が切り替わる（鍵更新を実施する）。そして、車載機が自身の判断により鍵更新へ状態が切り替わったり、鍵更新を要求することはない。また、この認証方式を実施する路側機は、車載機に対して鍵情報を要求及びチェックし、必要であれば鍵更新を車載機に指示する。すなわち、路側機主導で処理が行なわれる。

【００５８】

また、ここでは、一例として、ＥＴＣ、ドライブスルー等での自動車（車載機）と路側機（店舗システム）とに適用し、想定したが、通信装置は限定するものではない。例えば、基地局と携帯電話、無線ＬＡＮ（基地局とパソコン）、Ｒ／Ｗ（リーダー／ライター）とＲＦ　Ｔａｇ（電子タグ）といった固定局と移動局とにおける通信はもちろんのこと、モバイルとモバイルの通信等にも適用できる。

【００５９】

以上のように、本実施の形態によれば、鍵なし・期限切れ等の場合であっても鍵の更新をおこなうことができ、その後に正当な利用者がサービスの提供を受けることができ、本発明を利用するシステムのサービスの可用性及び利用者の利便性を向上させることができる。

【００６０】

また、本実施の形態によれば、さらに、セットアップ作業が不要となる。具体的には、例えば、車載機の出荷時及び店舗にて自動車に設置時、暗号通信に用いる鍵等車載機固有情報のセットアップが不要となる。そのため、製造においては同一の車載機を生産することができ生産効率が向上する。車載機固有の情報は、システムのセキュリティを維持するために重要なものであるため、セットアップ時の固有情報の取得は登録・作業者の限定といった細かな制限事項が発生する。しかし、セットアップ作業が不要なためどの業者でも設置でき流通コスト及び作業が軽減される。

【００６１】

実施の形態２．

図８は、実施の形態２における鍵更新処理に至るまでの手順を示すフローチャート図である。

【００６２】

Ｓ８０１において、認証処理部１９７は、被認証装置となる通信装置２００との間で認証処理をおこなう。言い換えれば、認証処理部２９７は、認証装置となる通信装置１００との間で認証処理をおこなう。認証処理の際、認証用鍵を用いておこなう。ここで、記憶部２２０が、古くなった或いは使用期限が過ぎた認証用鍵を記憶している場合、或いは、記憶部２２０が、認証用鍵を記憶していない場合、認証用鍵が使用できないので、ここでの認証処理は失敗に終わることになる。

【００６３】

Ｓ８０２において、送信部１１２は、認証処理が失敗に終わったことを示す失敗データを通信装置２００に送信する。

【００６４】

Ｓ８０３において、受信部２１１は、通信装置１００より失敗データを受信する。

【００６５】

Ｓ８０４において、送信部２１２は、失敗データを受信したことを示す確認データ（Ａｃｋ）を通信装置１００に送信（返信）する。

【００６６】

Ｓ８０５において、通信装置１００は、図３に示す鍵更新方法による鍵更新処理を開始する。

【００６７】

実施の形態１では、認証処理部１９７が、認証処理が失敗に終わったと判断した場合に、直ちに図３に示す鍵更新方法による鍵更新処理を開始するが、図８に示すように、認証処理が失敗に終わったことを通信装置１００，２００間で確認した後に鍵更新方法による鍵更新処理を開始するようにしてもよい。

【００６８】

図９は、ハードウェア構成図である。

【００６９】

以上の説明において、各実施の形態の説明において「～部」として説明したものを、一部或いはすべてコンピュータで動作可能なプログラムにより構成する場合、図９に示すように、通信装置１００，２００は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）３７を備えている。ＣＰＵ３７は、内蔵された、或いはバス３８を介してＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）４０（記憶装置、記憶部の一例である）、外部と通信可能な通信ポート４４に接続されている。また、図９に示すように、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）３９、磁気ディスク装置４６等の記憶装置に接続されていても構わない。

【００７０】

プログラムにより構成する場合、図９におけるプログラム群４９には、各実施の形態の説明において「～部」として説明したものにより実行されるプログラムが記憶されている。プログラム群４９は、上記記憶装置に記憶されている。プログラム群４９は、ＣＰＵ３７、ＯＳ４７等により実行される。記憶装置は、各処理の結果を記憶する。

【００７１】

また、各実施の形態の説明において「～部」として説明したものは、ＲＯＭ３９に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

【００７２】

また、上記各実施の形態を実施させるプログラムは、ＦＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ）、光ディスク、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）等のその他の記録媒体による記録装置を用いて記憶されても構わない。係る場合には、図９に示すように、ＦＤＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ　Ｄｒｉｖｅ）４５、コンパクトディスク装置（ＣＤＤ）８６等を備える。

【産業上の利用可能性】

【００７３】

このような通信装置１００，２００は、ＥＴＣ、ドライブスルー等における店舗側の路側機と自動車側の車載機に限らず、携帯電話等の移動体通信装置間、有線の通信装置間、或いは基地局を経由した有線と無線の通信装置間等における認証装置、被認証装置として、使用することができる。

【図面の簡単な説明】

【００７４】

【図１】実施の形態１における認証システムの構成を示す図である。

【図２】実施の形態１における認証システムの概念を示す図である。

【図３】実施の形態１における鍵更新方法の手順を示すフローチャート図である。

【図４】通信情報１のフレームの一例を示す図である。

【図５】通信情報２のフレームの一例を示す図である。

【図６】通信情報３のフレームの一例を示す図である。

【図７】通信情報４のフレームの一例を示す図である。

【図８】実施の形態２における鍵更新処理に至るまでの手順を示すフローチャート図

である。

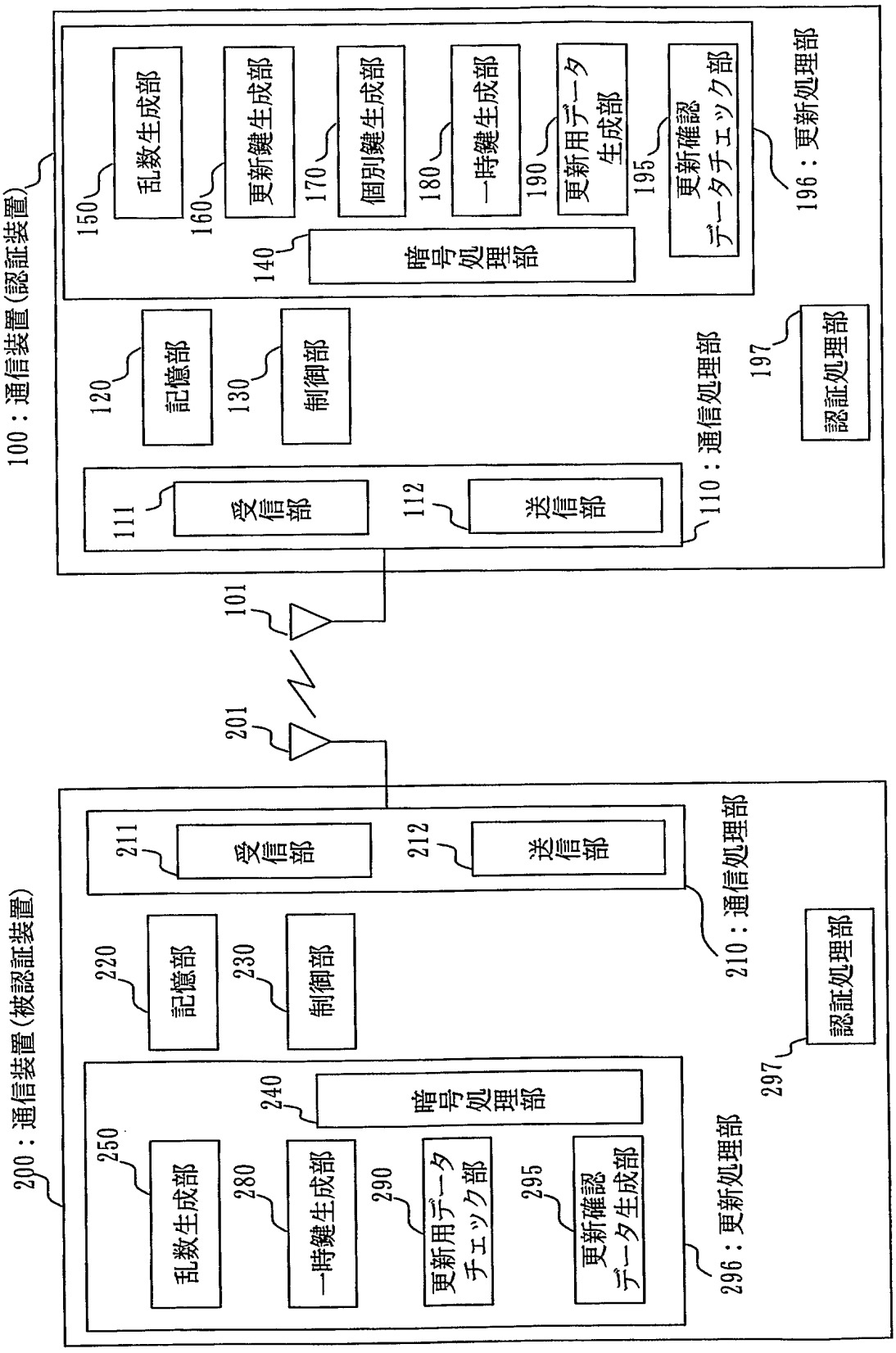
【図９】ハードウェア構成図である。

【符号の説明】

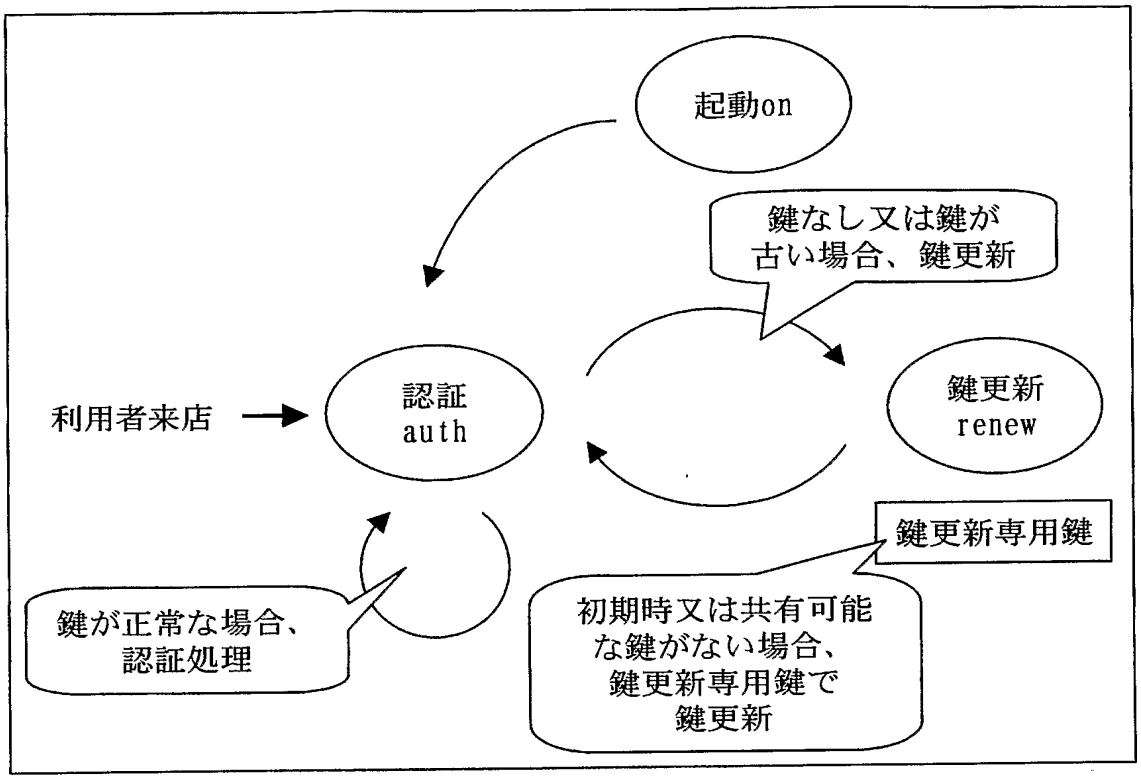
【００７５】

３７　ＣＰＵ、３８　バス、３９　ＲＯＭ、４０　ＲＡＭ、４４　通信ポート、４５　ＦＤＤ、４６　磁気ディスク装置、４７　ＯＳ、４９　プログラム群、８６　ＣＤＤ、１００　通信装置、１０１　アンテナ、１１０　通信処理部、１１１　受信部、１１２　送信部、１２０　記憶部、１３０　制御部、１４０　暗号処理部、１５０　乱数生成部、１６０　更新鍵生成部、１７０　個別鍵生成部、１８０　一時鍵生成部、１９０　更新用データ生成部、１９５　更新確認データチェック部、１９６　更新処理部、１９７　認証処理部、２００　通信装置、２０１　アンテナ、２１０　通信処理部、２１１　受信部、２１２　送信部、２２０　記憶部、２３０　制御部、２４０　暗号処理部、２５０　乱数生成部、２８０　一時鍵生成部、２９０　更新用データチェック部、２９５　更新確認データ生成部、２９６　更新処理部、２９７　認証処理部。

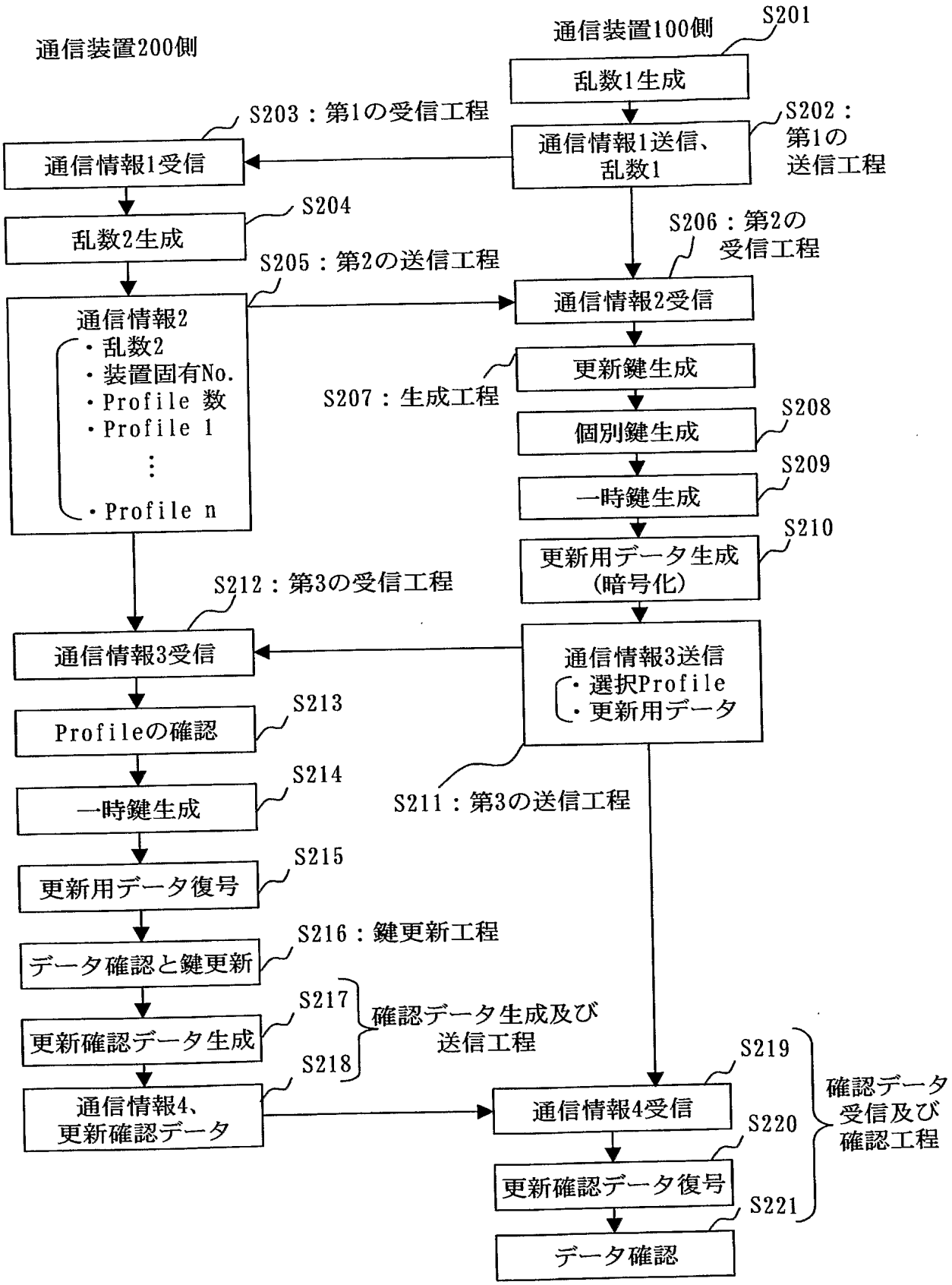
【書類名】図面
【図１】


100：通信装置(認証装置)
150
乱数生成部
160
更新鍵生成部
170
個別鍵生成部
180
一時鍵生成部
190
更新用データ生成部
195
更新確認データチェック部
196：更新処理部
140
暗号処理部
120
記憶部
130
制御部
111
受信部
112
送信部
110：通信処理部
197
認証処理部
101
201
200：通信装置(被認証装置)
211
受信部
212
送信部
210：通信処理部
220
記憶部
230
制御部
240
暗号処理部
250
乱数生成部
280
一時鍵生成部
290
更新用データチェック部
295
更新確認データ生成部
296：更新処理部
297
認証処理部

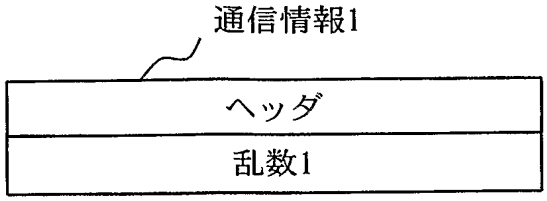
【図２】


起動on
鍵なし又は鍵が
古い場合、鍵更新
利用者来店
認証
auth
鍵更新
renew
鍵更新専用鍵
鍵が正常な場合、
認証処理
初期時又は共有可能
な鍵がない場合、
鍵更新専用鍵で
鍵更新

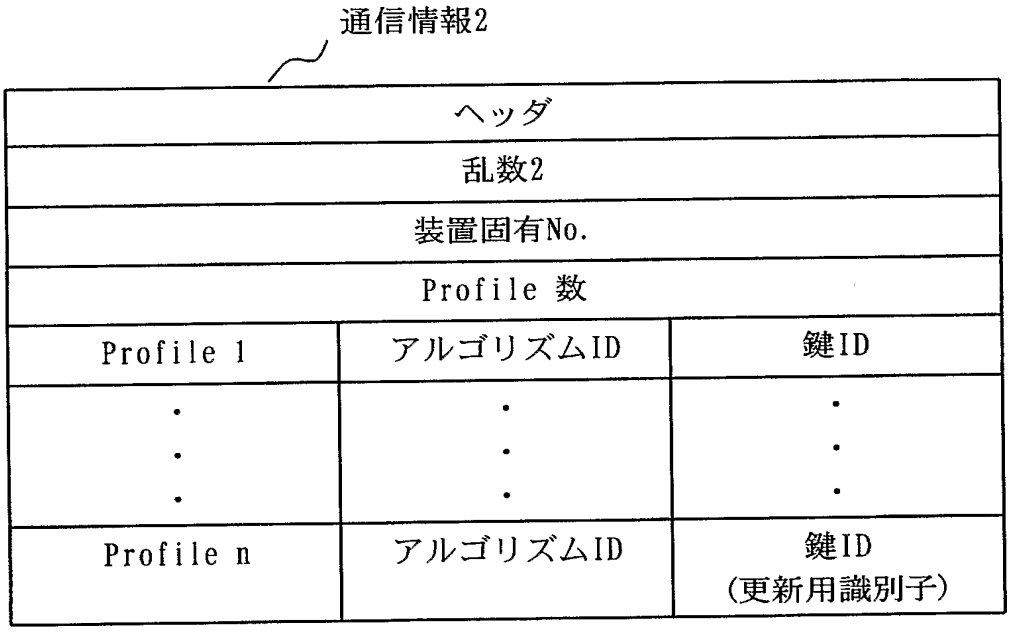
【図３】


通信装置200側
通信装置100側
S201
乱数1生成
S203：第1の受信工程
通信情報1受信
通信情報1送信、
乱数1
S202：
第1の
送信工程
S204
乱数2生成
S206：第2の
受信工程
S205：第2の送信工程
通信情報2
・乱数2
・装置固有No.
・Profile 数
・Profile 1
・Profile n
通信情報2受信
更新鍵生成
S207：生成工程
S208
個別鍵生成
S209
一時鍵生成
S210
更新用データ生成
(暗号化)
S212：第3の受信工程
通信情報3受信
通信情報3送信
・選択Profile
・更新用データ
S213
Profileの確認
S214
一時鍵生成
S211：第3の送信工程
S215
更新用データ復号
S216：鍵更新工程
データ確認と鍵更新
S217
更新確認データ生成
確認データ生成及び
送信工程
S218
通信情報4、
更新確認データ
S219
通信情報4受信
確認データ
受信及び
確認工程
S220
更新確認データ復号
S221
データ確認

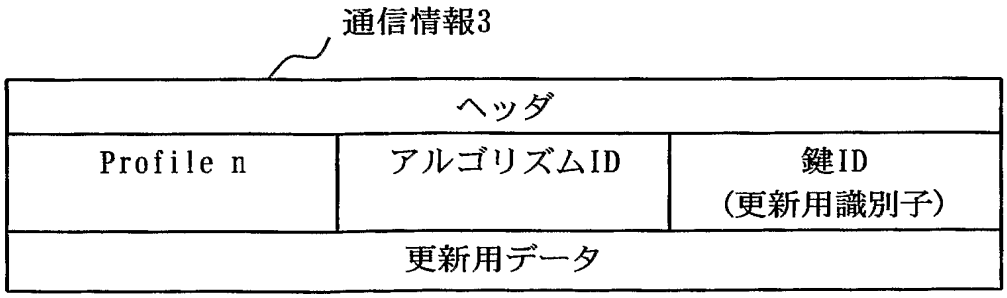
【図４】


通信情報1
ヘッダ
乱数1

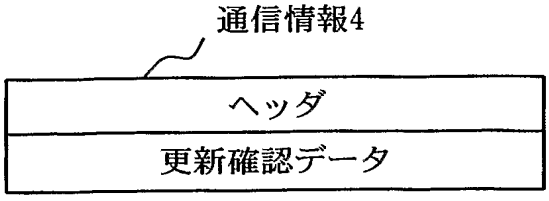
【図５】


通信情報2
ヘッダ
乱数2
装置固有No.
Profile 数
Profile 1
アルゴリズムID
鍵ID
Profile n
アルゴリズムID
鍵ID
(更新用識別子)

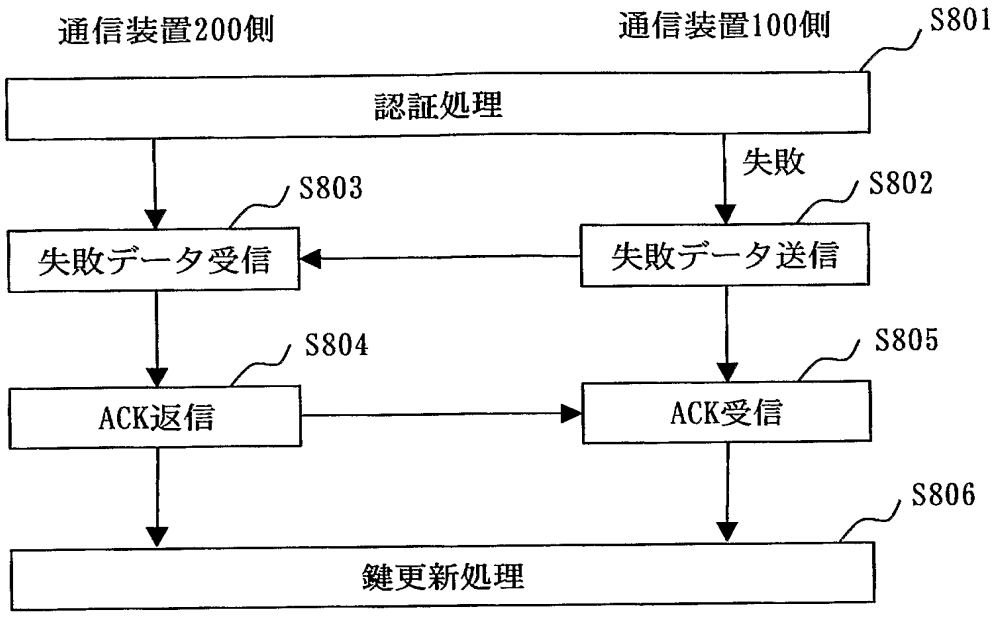
【図６】


通信情報3
ヘッダ
Profile n
アルゴリズムID
鍵ID
(更新用識別子)
更新用データ

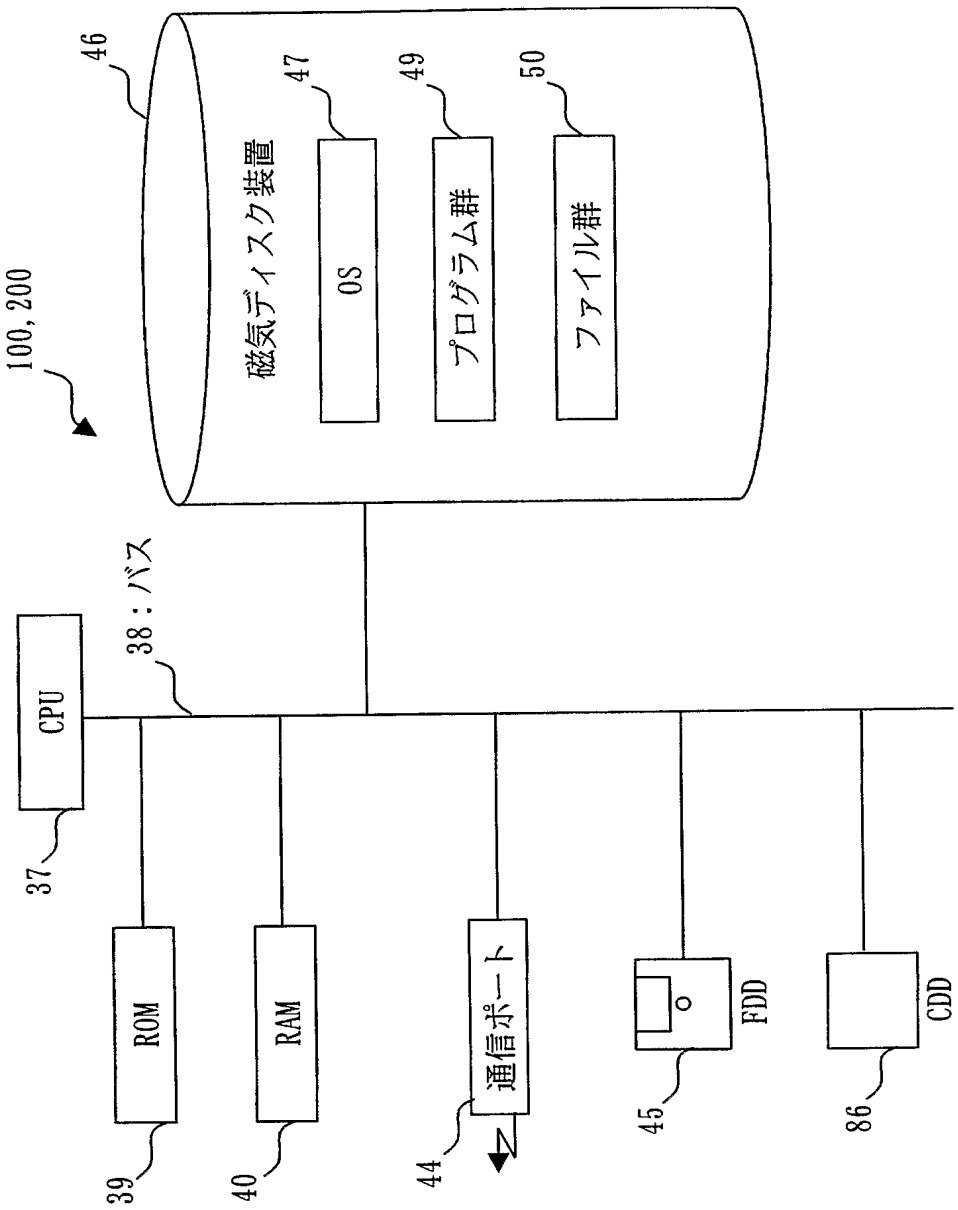
【図７】


通信情報4
ヘッダ
更新確認データ

【図８】


通信装置200側
通信装置100側
S801
認証処理
失敗
S803
S802
失敗データ受信
失敗データ送信
S804
S805
ACK返信
ACK受信
S806
鍵更新処理

【図９】


46
磁気ディスク装置
47
OS
49
プログラム群
50
ファイル群
100, 200
38：バス
CPU
37
ROM
39
RAM
40
通信ポート
44
FDD
45
CDD
86

【書類名】要約書
【要約】
【課題】　鍵更新をおこなうことで更新された鍵により正当な利用者に対しては、サービスを提供し、サービスの可用性及び利用者の利便性を向上させることを目的とする。
【解決手段】　認証用鍵を用いて通信装置２００との間で認証処理をおこなう認証処理部１９７と、上記認証処理部１９７による認証処理に用いる認証用鍵を通信装置２０が保持していない場合に新たな認証用鍵を生成し、上記通信装置２００が保持している場合で上記認証処理部１９７による通信装置２００との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部１６０とを備え、上記認証処理部１９７は、上記更新鍵生成部１６０により生成された新たな認証用鍵を用いて通信装置２００との間での認証処理を再度おこなうことを特徴とする。
【選択図】　図１

特願２００３－４３２４４７

出　願　人　履　歴　情　報

識別番号　［０００００６０１３］

１．変更年月日　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社